CLAIMS

WE CLAIM:

1. A circuit for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels, the circuit comprising:

round key generation means for (i) selectively receiving a cipher key and (ii) generating a round key of a first predetermined bit length from the received cipher key a predetermined number of times based on the AES Rijndael key expansion algorithm;

encryption/decryption means for (i) selectively receiving a data block of the first predetermined bit length from one of the plurality of system channels and a round key from the round key generation means and (ii) encrypting/decrypting the received data block a predetermined number of rounds based on the AES block cipher algorithm; and

controller means, responsive to control signals from each of the plurality of system channels, for controlling the round key generation means and the encryption/decryption means to selectively encrypt or decrypt the data block from individual ones of the plurality of system channels in a round-robin fashion.

2. The circuit of Claim 1, further comprising:

a plurality of cipher key storage means, one coupled to each of the plurality of system channels, for (i) storing a cipher key received from one of the system channels and (ii) transmitting the cipher key to the round key generation means.

3. The circuit of Claim 1, further comprising:

buffer register means for (i) selectively receiving and concatenating a plurality of data strings of a second predetermined bit length from one of the plurality of system channels and (ii) transmitting the concatenated data strings to the encryption/decryption means as the data block of the first predetermined bit length.

4. The circuit of Claim 3, further comprising:

a plurality of input means, one coupled to each of the plurality of system channels, for receiving the data strings of the second predetermined bit length from the plurality of system channels and (ii) selectively transmitting the data strings to the buffer register means.

5. The circuit of Claim 1, further comprising:

a plurality of cipher text storage means, one associated with each of the plurality of system channels, for selectively receiving an encrypted/decrypted data block of the first predetermined bit length from the encryption/decryption means.

6. The circuit of Claim 5, further comprising:

a plurality of output means, one coupled to each of the plurality of system channels, for selectively receiving an encrypted/decrypted data string of the second predetermined bit length from one of the plurality of cipher text storage means,

wherein the encrypted/decrypted data strings are portions of the encrypted/decrypted data blocks of the first predetermined bit length.

7. The circuit of Claim 1, further comprising:

plaintext processing means for (i) selectively receiving a data string of the second predetermined bit length from one of the plurality of system channels and (ii) transmitting the received data string, unaltered, to one of the plurality of system channels.

8. The circuit of Claim 1, wherein the encryption/decryption means comprises:

bytesub/invbytesub means, responsive to the controller means, for transforming the received data string according to either the ByteSub or InvByteSub function, as defined by the AES block cipher algorithm;

shiftrow/invshiftrow means, coupled to receive data from the bytesub/invbytesub means, and being responsive to the controller means, for transforming the received data according either the ShiftRow or InvShiftRow function, as defined by the AES block cipher algorithm; and

mixcol/invmixcol means, coupled to receive data from the shiftrow/invshiftrow means, and being responsive to the controller means, for transforming the received data according to either the MixCol or InvMixCol function, as defined by the AES block cipher algorithm.

9. The circuit of Claim 8, wherein the bytesub/invbytesub means comprises:

inverse affine means for receiving a vector data byte and performing an inverse affine transformation thereon to generate a transformed vector data byte;

first data switching means for:

(i) receiving the vector data byte, the transformed vector data byte, and an encrypt/decrypt control signal; and

(ii) transmitting the vector data byte when the control signal indicates the circuit is in an encrypt state and transmitting the transformed vector data byte when the control signal indicates the circuit is in a decrypt state;

inverse vector data byte determination means for:

(i) selectively receiving one of the vector data byte and the transformed vector data byte, in accordance with the control signal received by the first data switching means; and

(ii) determining an inverse vector data byte;

affine transformation means for receiving the inverse vector byte and applying an affine transformation thereon to generate a transformed inverse vector data byte; and

second data switching means for:

(i) receiving the inverse vector data byte, the transformed inverse vector data byte, and the encrypt/decrypt control signal; and

(ii) transmitting the inverse vector data when the control signal indicates the circuit is in an encrypt state and transmitting the transformed inverse vector data byte when the control signal indicates the circuit is in a decrypt state.

10. The circuit of Claim 1, wherein the round key generation means:

generates a round key one time during each round of the AES block cipher algorithm.

11. The circuit of Claim 10, wherein the each round key is generated according to the following algorithm:

New_W0 = Old_W0 XOR Kf(Old_W(nk-1);

New_W1 = Old_W1 XOR New_W0;

.

.

.

New_W(nk-1) = Old_W(nk-1) XOR New_W(nk-2);

where, nk=key size; nb=block size; and Kf is a function defined in the Rindeal block cipher specification,

wherein for nk=8 the above algorithm is modified as follows:

New_W4 = Old _W4 XOR ByteSub(New_W3).

12. The circuit of Claim 2, further comprising:

a plurality of final round key storage means, one in each of the plurality of system channels, for storing a key used for a final encryption round, as defined by the AES block cipher algorithm,

wherein the cipher key storage means in each channel, responsive to the controller means, retrieves the stored key for use in a first decryption round, as defined by the AES block cipher algorithm, and

wherein each round key used in subsequent decryption rounds is generated from the round key used in a previous decryption round.

13 The circuit of Claim 1, further comprising:

CBC implementation means, responsive to the controller means, for implementing a CBC encryption mode.

14. The circuit of Claim 13, wherein the CBC implementation means comprises:

initial value storage means for storing an initial round value; and

exclusive-OR means, responsive to the controller means, for receiving the stored initial value and XORing it with a value of a proceeding round.

15. The circuit of Claim 1, wherein a combination of the first predetermined bit length/ predetermined number of times is selected from the group consisting of 128/10, 192/12, and 256/14.

16. A circuit for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels, the circuit comprising:

a plurality of cipher key storage means, one coupled to each of the plurality of system channels, for storing a cipher key received from one of the system channels;

buffer register means for selectively receiving and concatenating a plurality of data strings of a first predetermined bit length from one of the plurality of system channels into a data block of a second predetermined bit length.

round key generation means for (i) selectively receiving one of the stored cipher keys from one of the plurality of cipher key storage means and (ii) generating a round key of the second predetermined bit length from the received cipher key a predetermined number of times based on the AES Rijndael key expansion algorithm;

encryption/decryption means for (i) selectively receiving a data block of the second predetermined bit length from the buffer register means and a round key from the round key generation means and (ii) encrypting/decrypting the received data block a predetermined number of rounds based on the AES block cipher algorithm; and

controller means, responsive to control signals from each of the plurality of system channels, for controlling the round key generation means and the encryption/decryption means to selectively encrypt or decrypt a data block from individual ones of the plurality of system channels in a round-robin fashion.

17 The circuit of Claim 16, further comprising:

a plurality of input means, one coupled to each of the plurality of system channels, for receiving (i) the data strings of the first predetermined bit length from the plurality of system channels and (ii) selectively transmitting the data strings to the buffer register means.

18. The circuit of Claim 16, further comprising:

a plurality of cipher text storage means, one associated with each of the plurality of system channels, for selectively receiving an encrypted/decrypted data block of the second predetermined bit length from the encryption/decryption means.

19. The circuit of Claim 18, further comprising:

a plurality of output means, one coupled to each of the plurality of system channels, for selectively receiving an encrypted/decrypted data string of the first predetermined bit length from one of the plurality of cipher text storage means,

wherein the encrypted/decrypted data strings are portions of the encrypted/decrypted data blocks of the second predetermined bit length.

20. The circuit of Claim 16, further comprising:

plaintext processing means for (i) selectively receiving a data string of the first predetermined bit length from one of the plurality of system channels and (ii) transmitting the received data string, unaltered, to one of the plurality of system channels.

21. The circuit of Claim 16, wherein the encryption/decryption means comprises:

bytesub/invbytesub means being responsive to the controller means for transforming the received data block according to either the ByteSub or InvByteSub function, as defined by the AES block cipher algorithm;

shiftrow/invshiftrow means, coupled to receive data from the bytesub/invbytesub means, and being responsive to the controller means for transforming the received data according either the ShiftRow or InvShiftRow function, as defined by the AES block cipher algorithm; and

mixcol/invmixcol means, coupled to receive data from the shiftrow/invshiftrow means and being responsive to the controller means for transforming the received data according to either the MixCol or InvMixCol function, as defined by the AES block cipher algorithm.

22. The circuit of Claim 21, wherein the bytesub/invbytesub means comprises:

inverse affine means for receiving a vector data byte and performing an inverse affine transformation thereon to generate a transformed vector data byte;

first data switching means for:

(i) receiving the vector data byte, the transformed vector data byte, and an encrypt/decrypt control signal; and

(ii) transmitting the vector data byte when the control signal indicates the circuit is in an encrypt state and transmitting the transformed vector data byte when the control signal indicates the circuit is in a decrypt state;

inverse vector data byte determination means for:

(i) selectively receiving one of the vector data byte and the transformed vector data byte, in accordance with the control signal received by the first data switching means; and

(ii) determining an inverse vector data byte;

affine transformation means for receiving the inverse vector byte and applying an affine transformation thereon to generate a transformed inverse vector data byte; and

second data switching means for:

(i) receiving the inverse vector data byte, the transformed inverse vector data byte, and the encrypt/decrypt control signal; and

(ii) transmitting the inverse vector data when the control signal indicates the circuit is in an encrypt state and transmitting the transformed inverse vector data byte when the control signal indicates the circuit is in a decrypt state.

23. The circuit of Claim 16, wherein the round key generation means:

generates a round key one time during each round of the AES block cipher algorithm.

24. The circuit of Claim 23, wherein the each round key is generated according to the following algorithm:

New_W0 = Old_W0 XOR Kf(Old_W(nk-1);

New_W1 = Old_W1 XOR New_W0;

.

.

.

New_W(nk-1) = Old_W(nk-1) XOR New_W(nk-2);

where, nk=key size; nb=block size; and Kf is a function defined in the Rindeal block cipher specification,

wherein for nk=8 the above algorithm is modified as follows:

New_W4 = Old _W4 XOR ByteSub(New_W3).

25. The circuit of Claim 16, further comprising:

a plurality of final round key storage means, one in each of the plurality of system channels, for storing a key used for a final encryption round, as defined by the AES block cipher algorithm,

wherein the cipher key storage means in each channel, responsive to the controller means, retrieves the stored key for use in a first decryption round, as defined by the AES block cipher algorithm, and

wherein each round key used in subsequent decryption rounds is generated from the round key used in a previous decryption round.

26. The circuit of Claim 16, further comprising:

CBC implementation means, responsive to the controller means, for implementing a CBC encryption mode.

27. The circuit of Claim 26, wherein the CBC implementation means comprises:

initial value storage means for storing an initial round value; and

exclusive-OR means, responsive to the controller means, for receiving the stored initial value and XORing it with a value of a proceeding round.

28. The circuit of Claim 16, wherein a combination of the second predetermined bit length/ predetermined number of times is selected from the group consisting of 128/10, 192/12, and 256/14.

29. A circuit for selectively determining S-box and inverse S-box data substitution values for a data string, the substitution values being associated with the

ByteSub and InvByteSub functions, respectively, of the Advanced Encryption Standard (AES) block cipher algorithm, the circuit comprising:

inverse affine means for receiving a vector data byte and performing an inverse affine transformation thereon to generate a transformed vector data byte;

first data switching means for:

(i) receiving the vector data byte, the transformed vector data byte, and an encrypt/decrypt control signal; and

(ii) transmitting the vector data byte when the control signal indicates the circuit is in an encrypt state and transmitting the transformed vector data byte when the control signal indicates the circuit is in a decrypt state;

inverse vector data byte determination means for:

(i) selectively receiving one of the vector data byte and the transformed vector data byte, in accordance with the control signal received by the first data switching means; and

(ii) determining an inverse vector data byte;

affine transformation means for receiving the inverse vector byte and applying an affine transformation thereon to generate a transformed inverse vector data byte; and

second data switching means for:

(i) receiving the inverse vector data byte, the transformed inverse vector data byte, and the encrypt/decrypt control signal; and

(ii) transmitting the inverse vector data when the control signal indicates the circuit is in an encrypt state and transmitting the transformed inverse vector data byte when the control signal indicates the circuit is in a decrypt state.

30. The circuit of Claim 29, wherein the vector data byte, or the transformed vector data byte, multiplied by the inverse vector data byte is an identity matrix modulo an irreducible polynomial in $GF(2^8)$.

31. The circuit of Claim 29, wherein the irreducible polynomial is:

$$x^8 + x^4 + x^3 + x + 1.$$

32. The circuit of Claim 29, wherein the first and second data switching means each comprise a multiplexer.

33. A method of efficiently generating round keys on-the-fly for use in decryption rounds of the AES cipher block algorithm, comprising:

generating a key used to encrypt a block of data in a final encryption round of the AES algorithm;

storing the generated key;

retrieving the stored key; and

generating a new key for use in each subsequent decryption round, without storing the new key each time one is generated and used.

34. The method of Claim 33, wherein the step of generating the key used to encrypt a block of data in the final encryption round is implemented in response to a specific command.

35. The method of Claim 33, wherein the new key is generated according to the following algorithm:

New_W(nk-1) = Old_W(nk-1) XOR Old_W(nk-2);
New_W(nk-2) = Old_W(nk-2) XOR Old_W(nk-3);

.

.

.

New_W0 = Old_W0 XOR Kf(New_W(nk-1),

where, nk=key size; nb=block size; and Kf is the function defined in the Rindeal block cipher specification,

wherein for nk=8the above algorithm is modified as follows:

New_W4 = Old_W4 XOR ByteSub(Old_W3).

36. A circuit for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels, the circuit comprising:

a plurality of cipher key storage means, one coupled to each of the plurality of system channels, for storing a cipher key received from one of the system channels;

buffer register means for selectively receiving and concatenating a plurality of data strings of a first predetermined bit length from one of the plurality of system channels into a data block of a second predetermined bit length;

round key generation means for (i) selectively receiving one of the stored cipher keys from one of the plurality of cipher key storage means and (ii) generating a round key of the second predetermined bit length from the received cipher key a predetermined number of times based on the AES Rijndael key expansion algorithm;

encryption/decryption means for (i) selectively receiving a data block of the second predetermined bit length from the buffer register means and a round key from the round key generation means and (ii) encrypting/decrypting the received data block a predetermined number of rounds based on the AES block cipher algorithm; and

controller means, responsive to control signals from each of the plurality of system channels, for controlling the round key generation means and the encryption/decryption means to selectively encrypt or decrypt a data block from individual ones of the plurality of system channels in a round-robin fashion,

wherein the encryption/decryption means comprises:

bytesub/invbytesub means for transforming the received data string according to either the ByteSub or InvByteSub function, as defined by the AES block cipher algorithm, based on the received control signal;

shiftrow/invshiftrow means, coupled to receive data from the bytesub/invbytesub mean, for transforming the received data according either the ShiftRow or InvShiftRow function, as defined by the AES block cipher algorithm, based on the received control signal; and

mixcol/invmixcol means, coupled to receive data from the shiftrow/invshiftrow means, for transforming the received data according to either the MixCol or InvMixCol function, as defined by the AES block cipher algorithm, based on the received control signal.

37. The circuit of Claim 36, wherein the bytesub/invbytesub means comprises:

inverse affine means for receiving a vector data byte and performing an inverse affine transformation thereon to generate a transformed vector data byte;

first data switching means for:

(i) receiving the vector data byte, the transformed vector data byte, and an encrypt/decrypt control signal; and

(ii) transmitting the vector data byte when the control signal indicates the circuit is in an encrypt state and transmitting the transformed vector data byte when the control signal indicates the circuit is in a decrypt state;

inverse vector data byte determination means for:

(i) selectively receiving one of the vector data byte and the transformed vector data byte, in accordance with the control signal received by the first data switching means; and

(ii) determining an inverse vector data byte;

affine transformation means for receiving the inverse vector byte and applying an affine transformation thereon to generate a transformed inverse vector data byte; and

second data switching means for:

(i) receiving the inverse vector data byte, the transformed inverse vector data byte, and the encrypt/decrypt control signal; and

(ii) transmitting the inverse vector data when the control signal indicates the circuit is in an encrypt state and transmitting the transformed inverse vector data byte when the control signal indicates the circuit is in a decrypt state.

38. A circuit for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels, the circuit comprising:

a round key generation circuit operable to (i) selectively receive a cipher key and (ii) generate a round key of a first predetermined bit length from the received cipher key a predetermined number of times based on the AES Rijndael key expansion algorithm;

an encryption/decryption circuit operable to (i) selectively receive a data block of the first predetermined bit length from one of the plurality of system channels and a round key from the round key generation circuit and (ii) encrypt/decrypt the received data block a predetermined number of rounds based on the AES block cipher algorithm; and

a controller, responsive to control signals from each of the plurality of system channels, operable to control the round key generation circuit and the encryption/decryption circuit to selectively encrypt or decrypt the data block from individual ones of the plurality of system channels in a round-robin fashion.

39. The circuit of Claim 38, further comprising:

a plurality of cipher key storage circuits, one coupled to each of the plurality of system channels, operable to (i) store a cipher key received from one of the system channels and (ii) transmit the cipher key to the round key generation circuit.

40. The circuit of Claim 38, further comprising:

a buffer register circuit operable to (i) selectively receive and concatenate a plurality of data strings of a second predetermined bit length from one of the plurality of system channels and (ii) transmit the concatenated data strings to the encryption/decryption circuit as the data block of the first predetermined bit length.

41. The circuit of Claim 40, further comprising:

a plurality of input circuits, one coupled to each of the plurality of system channels, operable to receive the data strings of the second predetermined bit length from the plurality of system channels and (ii) selectively transmit the data strings to the buffer register means.

42. The circuit of Claim 38, further comprising:

a plurality of cipher text storage circuits, one associated with each of the plurality of system channels, operable to selectively receive an encrypted/decrypted data block of the first predetermined bit length from the encryption/decryption circuit.

43. The circuit of Claim 42, further comprising:

a plurality of output circuits, one coupled to each of the plurality of system channels, operable to selectively receive an encrypted/decrypted data string of the second predetermined bit length from one of the plurality of cipher text storage circuits,

wherein the encrypted/decrypted data strings are portions of the encrypted/decrypted data blocks of the first predetermined bit length.

44. The circuit of Claim 38, further comprising:

a plaintext processing circuit operable to (i) selectively receive a data string of the second predetermined bit length from one of the plurality of system channels and (ii) transmit the received data string, unaltered, to one of the plurality of system channels.

45. The circuit of Claim 38, wherein the encryption/decryption circuit comprises:

a bytesub/invbytesub circuit operable in response to the controller circuit to transform the received data string according to either the ByteSub or InvByteSub function, as defined by the AES block cipher algorithm;

a shiftrow/invshiftrow circuit, coupled to receive data from the bytesub/invbytesub means, and being operable in respone to the controller circuit to transforme the received data according either the ShiftRow or InvShiftRow function, as defined by the AES block cipher algorithm; and

a mixcol/invmixcol circuit, coupled to receive data from the shiftrow/invshiftrow means, and being operable in response to the controller circuit to transform the received data according to either the MixCol or InvMixCol function, as defined by the AES block cipher algorithm.

46. The circuit of Claim 45, wherein the bytesub/invbytesub circuit comprises:

an inverse affine circuit operable to receive a vector data byte and perform an inverse affine transformation thereon to generate a transformed vector data byte;

a first data switching circuit operable to:

(i) receive the vector data byte, the transformed vector data byte, and an encrypt/decrypt control signal; and

(ii) transmit the vector data byte when the control signal indicates the circuit is in an encrypt state and transmit the transformed vector data byte when the control signal indicates the circuit is in a decrypt state;

an inverse vector data byte determination circuit operable to:

(i) selectively receive one of the vector data byte and the transformed vector data byte, in accordance with the control signal received by the first data switching circuit; and

(ii) determine an inverse vector data byte;

an affine transformation circuit operable to receive the inverse vector byte and apply an affine transformation thereon to generate a transformed inverse vector data byte; and

a second data switching circuit operable to:

(i) receive the inverse vector data byte, the transformed inverse vector data byte, and the encrypt/decrypt control signal; and

(ii) transmit the inverse vector data when the control signal indicates the circuit is in an encrypt state and transmit the transformed inverse vector data byte when the control signal indicates the circuit is in a decrypt state.

47. The circuit of Claim 38, wherein the round key generation circuit is operable to:

generate a round key one time during each round of the AES block cipher algorithm.

48. The circuit of Claim 47, wherein the each round key is generated according to the following algorithm:

New_W0 = Old_W0 XOR Kf(Old_W(nk-1);
New_W1 = Old_W1 XOR New_W0;
.
.
.
New_W(nk-1) = Old_W(nk-1) XOR New_W(nk-2);

where, nk=key size; nb=block size; and Kf is a function defined in the Rindeal block cipher specification,

wherein for nk=8 the above algorithm is modified as follows:

New_W4 = Old _W4 XOR ByteSub(New_W3).

49. The circuit of Claim 39, further comprising:

a plurality of final round key storage circuits, one in each of the plurality of system channels, operable to store a key used for a final encryption round, as defined by the AES block cipher algorithm,

wherein the cipher key storage circuit in each channel, responsive to the controller means, retrieves the stored key for use in a first decryption round, as defined by the AES block cipher algorithm, and

wherein each round key used in subsequent decryption rounds is generated from the round key used in a previous decryption round.

50. The circuit of Claim 38, further comprising:

a CBC implementation circuit, responsive to the controller, operable to implement a CBC encryption mode.

51. The circuit of Claim 50, wherein the CBC implementation circuit comprises:

an initial value storage circuit operable to store an initial round value; and

an exclusive-OR circuit, responsive to the controller, operable to receive the stored initial value and XOR it with a value of a proceeding round.

52. The circuit of Claim 38, wherein a combination of the first predetermined bit length/ predetermined number of times is selected from the group consisting of 128/10, 192/12, and 256/14.